University of Nottingham Rights Lab

GLOBAL FUND TO END MODERN SLAVERY

Legal and institutional responses to the online sexual exploitation of children

The Philippines country case study

September 2023

Content notice

This report deals with the topic of online sexual exploitation of children (OSEC) and includes reference to abuses experienced by children in this context. The report does not recount the specific experiences involved in OSEC cases. However, it does describe types and patterns of behaviour associated with OSEC in general terms.

Authorship and acknowledgements

This report was funded by the Global Fund to End Modern Slavery (GFEMS). The opinions, findings, and conclusions stated herein are those of the author(s) and do not necessarily reflect the views of GFEMS.

This report was reviewed by lived experience experts, whose inputs and perspectives are integrated throughout the document. Special thanks to Ruby, Liberty, and Joy for their invaluable insights. Special thanks to Ruby, Liberty, and Joy for reviewing and advising on this report.

Rights Lab project team

Dr Ergul Celiksoy, Rights Lab Research Fellow in Modern Slavery and Criminal Justice, University of Nottingham (lead author)

Dr Katarina Schwarz, Rights Lab Associate Director (Law and Policy) and Associate Professor of Antislavery Law and Policy, School of Law, University of Nottingham.

Contents

Figures

Tables

Table of abbreviations

AHTRAD	Anti-Human Trafficking Division
AMLC	Anti-Money Laundering Council
ATIPD	Anti-Trafficking in Persons Division
CIS	Customer Information Sheet
CSAEM	Child Sexual Abuse or Exploitation Materials
CSAM	Child Sexual Abuse Material
CSEM	Child Sexual Exploitation Material
DOJ-OCC	Department of Justice - Office of Cybercrime
ICTs	Information and Communication Technologies
IJM	International Justice Mission
ISPs	Internet Service Providers
KYSA	Know Your Sub-Agent
MSBs	Money Service Businesses
NBI	National Bureau of Investigation
NTC	National Telecommunications Commission
OSAEC	Online Sexual Abuse and Exploitation of Children
OSEC	Online Sexual Exploitation of Children
PHP	Philippine Pesos
PICACC	Philippine Internet Crimes Against Children Center
PNP	Philippine National Police
PNP-WCPC	Philippine National Police - Women and Children Protection Centre
PPPP	Public Private Partnership Program
PSPs	Payment System Providers
SIM	Subscriber Identity Module
STRs	Suspicious Transaction Reports
TIP	Trafficking in Persons
UNICEF	United Nations Children's Fund

Background

It is well-documented that children in the Philippines are subject to online sexual exploitation. The US Department of State 2022 TIP report found that children younger than 12 years old are forced to perform sexual acts in front of webcam (US Department of State, 2022). In March 2022, The Exodus Road—a non-profit organisation which works in collaboration with local law enforcement agencies tackling trafficking cases—reported that the Philippines is one of the major sources of online sexual exploitation of children (OSEC) (2022). Similarly, International Justice Mission (IJM) found that the Philippines is a global hotspot for OSEC (2020).

Not only is the Philippines a major source of OSEC, but cases in the country have been reported to have significantly increased in recent years. The Philippine Department of Justice observed the number of online sexual abuse and exploitation of children (OSAEC) cases increasing by 264% since the start of the Covid-19 pandemic(Watson, 2021). The Department of Justice – Office of Cybercrime (DOJ-OCC) reported a four-fold increase in the suspected incidence of OSAEC, from 76,559 in 2019 to 284,400 in 2020 (International Centre for Missing & Exploited Children, 2021, p. 8). Further, the Philippine Anti-Money Laundering Council (AMLC) reported that between 15 March and 15 May 2020, there were 5,902 OSEC related suspicious transaction reports (STRs), a considerable increase from the 369 SRTs during the same time frame in 2019 (AMLC, 2020, p. 14).

The financial motivation behind OSEC is apparent in most cases. This was confirmed by IJM gathering evidence from both the Philippines (in which 49 out of 59 investigation cases demonstrated clear financial motives) and international law enforcement referrals (where 53 out of 64 cases involved financial motives) (IJM, 2020, p. 56). Several other studies have also found that OSEC is mainly driven by financial motivations (ECPAT France, 2022; AMLC, 2020; Varrella, 2017; European Financial Coalition, 2015). Although the amount of money exchanged for OSEC varies considerably between cases, even the smallest exchange is usually equivalent to a substantial amount of money in the Philippines (IJM, 2020, p. 56). The lowest amount of money exchanged for OSEC is equal to several days, or even weeks, of wages in the Philippine. As such, poverty is considered as the primary reason for OSEC, as well as other child sex trafficking, in the country (ECPAT International, 2021). However, participants in this study highlighted that the increasing occurrence of live streamed OSEC in the Philippines cannot only be explained by poverty. Poverty is not the main driver for this sort of crime because the majority of economically struggling families do not resort to OSEC as a source of income (Interview #18).

Online sexual exploitation of children (OSEC) involves the use of technology and the internet to view and share child sexual exploitation material (CSEM), groom children online, or live stream sexual abuse of children. Abuse becomes exploitation where the offending involves an exchange of some kind of financial or other benefits. Generally, the offender pays through a money transfer agency to the trafficker who has access to exploited children to generate CSEM. This material is then transmitted from live streaming video communications platforms. These activities are classified as trafficking in persons according to the Palermo Protocol (IJM, 2020, p. 16). The Executive Director of IJM Center to End Online Sexual Exploitation of Children, John Tanagho summarised OSEC as follows:

> "The sex offender says 'I want to see a six-year-old girl sexually abused by an adult'. The trafficker says 'I can do that but I'm going to charge you'. [For example], The offender sitting in the UK wires the money and then they have a video call and that's when the child is sexually abused." – (Watson, 2021).

This report examines domestic legislation and policies relevant to OSEC in the Philippines, as well as exploring the investigation and prosecution of OSEC cases. Special attention is paid to financial flows involved in OSEC to analyse how payments made for OSEC are detected, reported, and investigated by the Filipino law enforcement agencies, other relevant domestic authorities, and the private sector.

1. Overview of domestic legislation and policy

The laws listed below are the primary legal instruments used by law enforcement and other domestic authorities when dealing with OSEC in the Philippines:

- Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act (Republic Act No. 11930)
- Anti-Child Pornography Act (Republic Act No. 9775)
- Expanded Anti-Trafficking in Persons Act (Republic Act No. 10364)
- Cybercrime Prevention Act (Republic Act No. 10175)
- Special Protection of Children Against Abuse, Exploitation and Discrimination Act (Republic Act No. 7610)
- Data Privacy Act (Republic Act No. 10173)
- Anti-Money Laundering Act (Republic Act No. 9160)
- Law on Secrecy of Bank Deposits (Republic Act No. 1405)
- Foreign Currency Deposit Act (Republic Act No. 6426

1.1. Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act (Republic Act No. 11930)

Enacted in 2022, the OSAEC and CSAEM Act of the Philippines provides a comprehensive framework for preventing and combatting the online sexual abuse and exploitation of children. The Act provides a definition of key terms and punishes a wide variety of acts of OSEC regardless of the consent of victims (children).

The OSAEC and CSAEM Act provides core definitions of a range of practices associated with OSEC.

- 'Child sexual abuse' is defined as any form of communication, physical interaction or activity between a child and any person that involves the use of the child for sexual gratification, regardless of the gender or consent of the victim (Section 3(b)).
- 'Child sexual exploitation' is defined, regardless of the consent of the child, as any acts of abuse or exploitation in exchange of something of value (whether monetary or non-monetary), or sexual intercourse with a child with or without consideration, or any other act related to child abuse, cruelty or exploitation (Section 3(d)).
- 'CSAEM/CSAM' is defined as any representation of a child involved in real or simulated sexual activities, or that depict sexual abuse or exploitation of a child as a sexual object. This includes material that focuses on a child's genitalia or other private body parts and can be represented in audio, visual, written or any combination thereof. This material can be stored and/or shared online or offline (Section 3(c)).
- 'Online sexual abuse or exploitation of children (OSAEC)' is defined as the use of technology to sexually abuse or exploit children. It includes scenarios where offline and online activities are combined, such as production, dissemination, and possession of child sexual abuse material (CSAEM). This includes online grooming for sexual purposes, sexual extortion, sharing image-based sexual abuse, commercial sexual exploitation of children, exploitation through online prostitution, and live streaming of sexual abuse (Section 3(t)).
- 'Image-based sexual abuse' is a form of technology-facilitated sexual violence, where non-consensual images are created, distributed, or threatened to be distributed. It includes a range of behaviours such as sextortion scams, deepfake porn and sexual assault imagery (Section 3(j)).

- 'Streaming' is defined the broadcasting or viewing of content through the use of information and communication technologies (ICTs), either passively or actively. It is considered live streaming when the broadcasting or viewing happens in real-time (Section 3(aa)).
- Also relevant to OSEC is 'grooming', which is defined as a form of predatory behaviour where someone establishes a relationship of trust with a child or someone believed to be a child, and/or their family, guardian and/or caregivers, in person or online, to perpetrate sexual abuse or exploitation or the production of any form of child sexual abuse material (Section 3(i)).
- 'Luring' is defined as the act of using a computer system to communicate with a child or someone the offender believes to be a child to facilitate the commission of sexual activity or production of any form of child sexual abuse material (Section 3(s)).
- 'Pandering' is defined as the act of offering, advertising, promoting, representing, or distributing material related to child sexual abuse or exploitation, regardless of its content (Section 3(u)).

The OSAEC and CSAEM Act provides a comprehensive framework in terms of punishable acts and penalties in relation of online sexual crimes against children. Table 1 summarises the acts punished under the OSAEC and CSAEM Act.

Table 1: Summary of offences and penalties in OSAEC and CSAEM Act

Penalty	Prohibited Acts
Life imprisonment + A fine of not less than PHP 2,000,000.00	▪ To hire, employ, use, persuade, induce, extort, engage, or coerce a child to perform or participate in whatever way in the creation or production of any form of OSAEC and CSAEM. ▪ To produce, direct, manufacture, facilitate, or create any form of CSAEM, or participate in the production, direction, manufacture, facilitation, or creation of the same. ▪ To offer, sell, distribute, advertise, promote, export, or import, by any means, any form of CSAEM. ▪ To knowingly publish, transmit, and broadcast, by any means, any form of CSAEM. ▪ To permit or influence the child to engage, participate, or assist in any form of CSAEM. ▪ To produce, direct, create, hire, employ, or pay a facilitator to stream or live stream acts of child sexual abuse or exploitation. ▪ To stream or live stream acts of, or any form of, child sexual abuse and exploitation. ▪ To recruit, transport, transfer, harbour, provide, or receive a child or to induce or influence the same, for the purpose of violating this Act. ▪ To introduce or match a child to a foreign national or to any person for the purpose of committing any of the offences under this Act. ▪ For film distributors, theatres, and ICT services by themselves or in cooperation with other entities, to distribute any form of CSAEM or to facilitate the commission of any of the offences under this Act.
Prison sentence from 17 years and 4 months to 20 years + A fine between PHP 1,000,000.00 and PHP 2,000,000.00.	▪ To knowingly benefit from, financial or otherwise, the commission of any of the offences of this Act ▪ To provide a venue for the commission of prohibited acts under this section such as dens, private rooms, cubicles, cinemas, houses, private homes, or other establishments
Prison sentence from 17 years and 4 months to 20 years +	▪ To engage in the luring or grooming of a child, including grooming taking place offline as a prelude to violations under this Act ▪ To sexualise children by presenting them as objects of sexual fantasy, or making them conversational subjects of sexual fantasies, in any online or digital platform

A fine between PHP 800,000.00 and PHP 1,000,000.00.	▪ To engage in pandering as defined under this Act
Prison sentence from 14 years and 8 months to 17 years and 4 months + A fine between PHP 500,000.00 and PHP 800,000.00.	▪ To wilfully subscribe, join, donate to, or support an internet site that hosts OSAEC or the streaming or live streaming of child sexual abuse and exploitation
Prison sentence from 12 years to 14 years and 8 months + A fine between PHP 300,000.00 and PHP 500,000.00.	▪ To advertise, publish, print, broadcast, or distribute, or cause the advertisement, publication, printing, broadcasting, or distribution by any means of any brochure, flyer, or any material that promotes OSAEC and child sexual abuse or exploitation
Prison sentence from 12 years to 20 years + A fine of not less than PHP 300,000.00.	▪ To possess any form of CSAEM, provided that possession of three (3) or more CSAEMs is prima facie evidence (on the face of evidence) of the intent to sell, distribute, publish, or broadcast
Prison sentence from 10 years to 12 years + A fine between PHP 200,000.00 and PHP 300,000.00.	▪ To wilfully access any form of CSAEM
Prison sentence from 8 years to 10 years + A fine between PHP 100,000.00 and PHP 200,000.00.	▪ To conspire to commit OSEC-related crimes stated in this section 4 of the Act
Life imprisonment + A fine between PHP 5,000,000.00 and PHP 20,000,000.00.	▪ If OSEC related crimes are committed by a syndicate (3 or more offenders) or in a large-scale (against 3 or more victims)

OSAEC and CSAEM Act appears to be designed in a way to address all aspects of online sexual crimes against children. Significantly, it imposes some obligations and duties on the private sector, including Internet Intermediaries, Internet Service Providers (ISPs), and Payment System Providers (PSPs).

Table 2: Duties and responsibilities of private sector actors in relation to combatting OSEC

Service Providers[1]	Duties
Internet Intermediaries	▪ Adopt products and services for the prohibition of any form or any conduct of streaming or live streaming of OSAEC and CSAEM in the use of their website, platform, server or facility ▪ Preserve all subscriber's or registration information and traffic data for up to 12 months ▪ Immediately block access to, remove or take down the internet address, URL, websites, or any content containing CSAEM or involving streaming or live streaming of OSAEC within 24 hours of notice ▪ Report to the Department of Justice within three days the internet address or websites blocked, removed, or taken down, or any form of unusual data activity using its server or facility ▪ Provide the Philippine National Police (PNP) with the subscriber's or registration information and/or traffic data of any person involved in CSAEM or streaming or live streaming of child sexual exploitation ▪ Develop, establish, and install mechanisms or measures designed to prevent, detect, respond, or report OSAEC, CSAEM, and streaming or live streaming of child sexual exploitation ▪ Coordinate with the Department of Justice-Office of Cybercrime
Internet Service Providers	▪ Internet Service Providers have all duties and responsibilities in relation to Internet Intermediaries listed above ▪ Notify the PNP or the National Bureau Investigation within 48 hours about child sexual abuse or exploitation committed using their server or facility, or is likely being committed using their server or facility ▪ Block CSAEM or the streaming or live streaming of a child sexually abused or exploited within 24 hours from receipt of notice ▪ Maintain logs of each and every subscriber and the IP address assigned to each and every subscriber at a given date and time ▪ Develop and adopt a set of systems and procedures for preventing, blocking, detecting, and reporting OSAEC and CSAEM committed within their platforms ▪ Adopt and integrate child protection standards in their corporate governance practice and processes ▪ Establish high privacy setting as default safety and privacy settings for children, and adopt age-verification controls and protocols
Payment System Providers	▪ Payment System Providers also have duties and responsibilities in relation to Internet Intermediaries listed above as far as they are relevant to them ▪ Any person with direct knowledge of any OSAEC and CSAEM financial activity should report any suspected OSAEC and CSAEM-related activity or suspicious transaction to the DOJ-OOC within 24 hours ▪ They should also report to the Anti-Money Laundering Council (AMLC) within 5 days ▪ Payment System Providers may be required to provide financial documents and information to law enforcement agencies ▪ Law enforcement agencies may inquire into or examine any particular deposit or investment, including related accounts, with any banking institution or any non-bank financial institution ▪ Money transfer and remittance centres shall require individuals transacting with them to present valid government identification cards

The OSAEC and CSAEM Act was welcomed by those working on OSEC investigation in the Philippines because it made it clear that Internet Intermediaries, ISPs, and PSPs have an obligation to address OSEC in their services and systems (Interview #18). The Act also clarified how law enforcement could make requests to get data from the private sector for the investigation and prosecution of OSEC crimes (ibid). Prior to the

[1] *Internet service providers (ISPs) supply internet access to individuals and commercial users. They range from large telecommunications providers to small resellers of capacity on a larger network (LexisNexis, n.d.). The term 'internet intermediaries' commonly refers to a wide, diverse and rapidly evolving range of service providers that facilitate interactions on the internet between natural and legal persons*
(Council of Europe, n.d.).

adoption of the Act, it was unclear whether law enforcement could request financial data from the financial sector. Under the OSAEC and CSAEM Act, law enforcement are able to make requests for financial data by court order (ibid).

Prior to the enactment of OSAEC and CSAEM Act, law enforcement agencies in the Philippines had to rely on other laws to investigate and prosecute online sexual crimes against children. For example, one respondent in a UNICEF study in 2020 stated that:

> "The thing with the present state of Philippine law is there's no specific penal statute that defines OSAEC or that penalizes OSAEC. You cannot find a Republic Act that defines online sexual exploitation of children. What we have are different laws on children others not specific to children that we use as legal basis in court…we are able to get convictions using these laws, so, in that regard they may be sufficient but the challenge is in a system that is not used to dealing with crimes or offenses that involve really young children, complicated by the use of the Internet and information and communications technology." - (UNICEF Philippines, 2020, p. 93).

Similarly, Noel Roa Eballe, Director of National Investigations and Law Enforcement Development at International Justice Mission in the Philippines, emphasised the importance of the OSAEC and CSAEM Act as follows:

> "For me, it has a tremendous impact on the fight against OSEC and the Philippines because it gives additional powers to Philippine law enforcement. It gives them more flexibility and it aids them as far as the investigative process would go in terms of investigating OSEC. It gives them more tools to investigate OSEC. So, to me, it has a tremendous effect on investigating OSEC cases in the Philippines and it is really an improvement as far as the Philippines situation is, as far as it relates to the work of law enforcement." - (Interview #18).

Although OSAEC and CSAEM Act provides a very comprehensive framework for the investigation and prosecution of online sexual crimes against children, its impact in practice remains to be seen, given that the law was just enacted in 2022.

1.2. Anti-Child Pornography Act (Republic Act No. 9775)

Section 3(a) & (b) and Section 4 of the Anti-Child Pornography Act provide a comprehensive definition of child sexual abuse material (CSAM) and make various forms of activity related to it a criminal offence.

Section 3 – Definition of Terms

(…)

(b) **"Child pornography"** refers to any representation, whether visual, audio, or written combination thereof, by electronic, mechanical, digital, optical, magnetic or any other means, of child engaged or involved in real or simulated explicit sexual activities.

(…)

(h) **"Grooming"** refers to the act of preparing a child or someone who the offender believes to be a child for sexual activity or sexual relationship by communicating any form of child pornography. It includes online enticement or enticement through any other means.

(i) **"Luring"** refers to the act of communicating, by means of a computer system, with a child or someone who the offender believes to be a child for the purpose of facilitating the commission of sexual activity or production of any form of child pornography.

(…)

The Anti-Child Pornography Act defines child pornography as visual, audio, and written representations that are stored through electronic and digital means (Section 3(b)). The possession of any form of child pornographic material with the intent to sell, distribute, publish, or broadcast is made illegal and is punishable under Section 4 of the Act.

The Anti-Child Pornography Act requires Internet Service Providers (ISPs) take actions to combat CSAM and child pornography (UNICEF Philippines, 2020, p. 88). Under the Anti-Child Pornography Act, ISPs are mandated to:

- Notify the Philippine National Police or the National Bureau of Investigation of any child pornography content in their server or facility within seven days of detection of such content.
- Preserve the relevant evidence of child pornography content for future investigation and prosecution by the relevant authorities.
- Provide authorities with the details and information of users who accessed or attempted to access an Internet address associated with any form of child pornography.
- Block and filter the access to or transmittal of any form of child pornography by installing available technology, programmes, or software (International Centre for Missing & Exploited Children, 2021, p. 12).

The implementation of these mandate has proven difficult in practice. NGOs and government organisations view these mandates as a call for ISPs to block websites containing child pornography, in an attempt to reduce OSEC (UNICEF Philippines, 2020, p. 88). However, ISPs argue that the software required for filtering is expensive and pose the question of who should be responsible for paying for it (ibid).

It should also be noted that acts punishable under Section of 4 of Anti-Child Pornography Act are predicate crimes under Section 3(i)(31) of the Anti-Money Laundering Act (see further section 2.8).

1.3. Expanded Anti-Trafficking in Persons Act (Republic Act No. 10364)

The Expanded Anti-Trafficking in Persons Act defines and punishes trafficking in persons in the Philippines. This piece of legislation is also relevant to OSEC because it punishes the using, procuring, or offering of a child for prostitution, for the production of pornography, or for pornographic performances.

> **Section 4: Acts of Trafficking in Persons**
>
> (…)
>
> (k) **To recruit, transport, harbor, obtain, transfer, maintain, hire, offer, provide, adopt or receive a child for purposes of exploitation or trading them, including but not limited to, the act of baring and/or selling a child for any consideration or for barter for purposes of exploitation. Trafficking for purposes of exploitation of children shall include:**
>
> (1) All forms of slavery or practices similar to slavery, involuntary servitude, debt bondage and forced labor, including recruitment of children for use in armed conflict;
>
> (2) The use, procuring or offering of a child for prostitution, for the production of pornography, or for pornographic performances;
>
> (3) The use, procuring or offering of a child for the production and trafficking of drugs; and
>
> (4) The use, procuring or offering of a child for illegal activities or work which, by its nature or the circumstances in which it is carried out, is likely to harm their health, safety or morals.
>
> (…)

The acts punishable under Section 4 of the Expanded Anti-Trafficking in Persons Act are predicate crimes under Section (3(i)(19) of the Anti-Money Laundering Act (see further section 2.8).

1.4. Cybercrime Prevention Act (Republic Act No. 10175)

The Cybercrime Prevention Act is known as the first law of its kind in the Philippines, providing a comprehensive overview of cybercrime and related offences, such as cybersex. This includes activities like interactive prostitution and pornography, for example when engaging in webcam or live streaming (International Centre for Missing & Exploited Children, 2021, p. 13).

> **Section 4: Cybercrime Offenses**
>
> (...)
>
> (c) **Content-related Offenses:**
>
> *(1)* **Cybersex.** — The willful engagement, maintenance, control, or operation, directly or indirectly, of any lascivious exhibition of sexual organs or sexual activity, with the aid of a computer system, for favor or consideration.
>
> *(2)* **Child Pornography.** — The unlawful or prohibited acts defined and punishable by Republic Act No. 9775 or the Anti-Child Pornography Act of 2009, committed through a computer system: Provided, That the penalty to be imposed shall be (1) one degree higher than that provided for in Republic Act No. 9775.
>
> (...)

The Cybercrime Prevention Act was enacted to address the issues posed by advances in technology. The law expanded the definition of child pornography to include any unlawful acts committed through a computer system and established a higher penalty when child pornography is committed through information and communication technologies (ICTs) (Section 6). In its interpretation of the Cybercrime Prevention Act, the Supreme Court of the Republic of the Philippines stated that:

> "Of course, the law makes the penalty higher by one degree when the crime is committed in cyberspace. But no one can complain since the intensity or duration of penalty is a legislative prerogative and there is rational basis for such higher penalty.32 The potential for uncontrolled proliferation of a particular piece of child pornography when uploaded in the cyberspace is incalculable." - (Supreme Court of the Republic of the Philippines, 2014).

1.5. Special Protection of Children Against Abuse, Exploitation and Discrimination Act (Republic Act No. 7610)

The Special Protection of Children Against Abuse, Exploitation and Discrimination Act is an important piece of legislation for the investigation and prosecution of online sexual crimes against children. This Act criminalises child prostitution and other sexual abuse, child trafficking, and other acts of abuse against children. Specifically, section 5 of the Act punishes hiring, employing, using, persuading, inducing, or coercing a child to perform in obscene exhibitions and indecent shows, whether live or in video. Further, sections 5, 7, 8, 9, 10 (c), 10 (d), 10 (e), 11, 12, and 14 of the Act are predicate crimes under the Anti-Money Laundering Act (Section 3(i)(32)) (see further section 2.8).

1.6. Data Privacy Act (Republic Act No. 10173)

The Data Privacy Act enforces the policy of the State to protect individuals' right to privacy by controlling the processing and transmission of personal information. The regulation applies to all types of personal information and to any individual or legal entity that is involved in the processing of this data, even to those who are not based in the Philippines but use equipment located there, or who have an office, branch, or agency in the country, with some exceptions. The Data Privacy Act requires banks and other financial institutions that are regulated by the Bangko Sentral ng Pilipinas to comply with the requirements of the Anti-Money Laundering Act and any other applicable laws (International Centre for Missing & Exploited Children, 2021, p. 30).

1.7. Subscriber Identity Module (SIM) Registration Act (Republic Act No. 11934)

In October 2022, the Philippines passed Republic Act No. 11934, also known as the Subscriber Identity Module (SIM) Registration Act. This act mandates the registration of all mobile phone subscribers before they can use their device. The purpose of this law is to reduce the number of unregistered SIM cards and to help law enforcement agencies track down criminals. Under the SIM Registration Act, all mobile phone users must register their SIM card with their mobile phone service provider. This includes providing personal information such as name, address, and date of birth, as well as a valid ID. The mobile phone service provider will then send this information to the National Telecommunications Commission (NTC). Once a SIM card is registered, the NTC will provide a unique identification number for the SIM card. This number will be linked to the subscriber's name and other personal information. The SIM Registration Act also requires mobile phone service providers to keep records of all registered SIM cards. These records must be kept for at least five years and must be made available to law enforcement agencies upon request.

The SIM Registration Act can be considered an important tool in identifying and investigating OSEC cases where facilitators use their mobile phone to commit the crimes. The Act provides law enforcement with an opportunity to trace back to a SIM card or mobile phone used for OSEC.

1.8. Anti-Money Laundering Act (Republic Act No. 9160)

The Anti-Money Laundering Act is an important tool to investigate and prosecute financial transactions involved in OSEC. It defines money laundering under section 4, as involving three distinct conducts: transacting proceeds of unlawful activity, facilitating such transactions, or failing to report to the Anti-Money Laundering Council (AMLC) established under the Act.

> **Section 4: Money Laundering Offense**
>
> Money laundering is a crime whereby the proceeds of an unlawful activity are transacted, thereby making them appear to have originated from legitimate sources. It is committed by the following:
>
> (a) Any person knowing that any monetary instrument or property represents, involves, or relates to, the proceeds of any unlawful activity, transacts or attempts to transact said monetary instrument or property.
>
> (b) Any person knowing that any monetary instrument or property involves the proceeds of any unlawful activity, performs or fails to perform any act as a result of which he facilitates the offense of money laundering referred to in paragraph (a) above.
>
> (c) Any person knowing that any monetary instrument or property is required under this Act to be disclosed and filed with the Anti-Money Laundering Council (AMLC), fails to do so.

The definition of money laundering includes specific types of 'unlawful activity', defined under section 3(i). These 'predicate crimes'—set out in Table 3—include conduct connected to OSEC.

The Anti-Money Laundering Act mandates that any person subject to its provisions must report any covered or suspicious transactions to the Anti-Money Laundering Council (AMLC) within five business days of them taking place.2 Additionally, the Act allows the AMLC to investigate deposits and investments with banks and non-bank financial institutions with the approval of a court, when it is thought that the deposits or investments are linked to an illegal activity or money laundering, notwithstanding any existing laws protecting bank secrecy.

Table 3: Provisions of laws considered 'unlawful activity' under Anti-Money Laundering Act

Laws	Provisions considered 'unlawful activity' under Anti-Money Laundering Act
Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act (Republic Act No. 11930)	Sections 4 and 5
Anti-Child Pornography Act (Republic Act No. 9775)	Section of 4
Expanded Anti-Trafficking in Persons Act (Republic Act No. 10364)	Section of 4
Special Protection of Children Against Abuse, Exploitation and Discrimination Act (Republic Act No. 7610)	Sections 5, 7, 8, 9, 10 (c), 10 (d), 10 (e), 11, 12, and 14
Cybercrime Prevention Act (Republic Act No. 10175)	N/A
Data Privacy Act (Republic Act No. 10173)	N/A
Law on Secrecy of Bank Deposits (Republic Act No. 1405)	N/A
Foreign Currency Deposit Act (Republic Act No. 6426)	N/A
Subscriber Identity Module (SIM) Registration Act (Republic Act No. 11934)	N/A

Established under the Anti-Money Laundering Act, the AMLC has a number of tools at its disposal to help combat OSEC, including:

- The exchange, distribution, and communication of financial intelligence, both domestically and internationally, to governmental entities (Section 7(8)).
- Filing complaints to the Department of Justice or the Ombudsman to initiate prosecution of money laundering offences (Section 7(4)).
- Initiating investigations of covered transactions and money laundering activities (Section 7(5)).
- Freezing any monetary instrument or property alleged to be proceeds of any unlawful activity (Section 7(6)).
- Ensuring mutual legal assistance with other countries (Section 13).

The AMLC has the power to inspect and acquire data concerning bank accounts related to unlawful activity, apart from certain exemptions. However, the Anti-Money Laundering Act does not provide a concrete foundation for the AMLC to hand over the data it has collected to law enforcement agencies for the purpose of examining or punishing any of the illegal activities (International Centre for Missing & Exploited Children, 2021, p. 25). Therefore, it is suggested that if there were a legally acceptable way for the AMLC to exchange information with law enforcement agencies, it would be easier to detect OSEC cases (ibid).

[2] *Rule 22, Section 2, of the 2018 Implementing Rules and Regulations of the Anti-Money Laundering Act.*

1.9. Law on Secrecy of Bank Deposits (Republic Act No. 1405) and Foreign Currency Deposit Act (Republic Act No. 6426)

The Law on Secrecy of Bank Deposits (Republic Act No. 1405) provides that all deposits with Philippine banks, regardless of what they may be, shall be kept confidential unless the depositor gives written consent, or in the event of impeachment, if a public official is accused of bribery or misconduct, or if the money deposited is the subject of a litigation. Similarly, the Foreign Currency Deposit Act (Republic Act No. 6426) provides that all currency deposits are confidential except upon the written permission of the depositors. These pieces of legislation may pose a challenge to law enforcement as they may not request information regarding a deposit into a bank account unless there is a written consent from the depositor or ongoing litigation. This impedes law enforcement efforts to build cases when investigating OSEC.

There are several exceptions to these laws as far as the Anti-Money Laundering Act is concerned. According to section 11 of the Anti-Money Laundering Act, the AMLC may inquire into or examine any particular deposit or investment with any banking institution or non-bank financial institution upon order of any competent court. Further, the Anti-Money Laundering Act repealed the provisions of Law on Secrecy of Bank Deposits and Foreign Currency Deposit Act, which are inconsistent with the Anti-Money Laundering Act (Section 22).

2. Investigation and prosecution of OSEC Cases in the Philippines

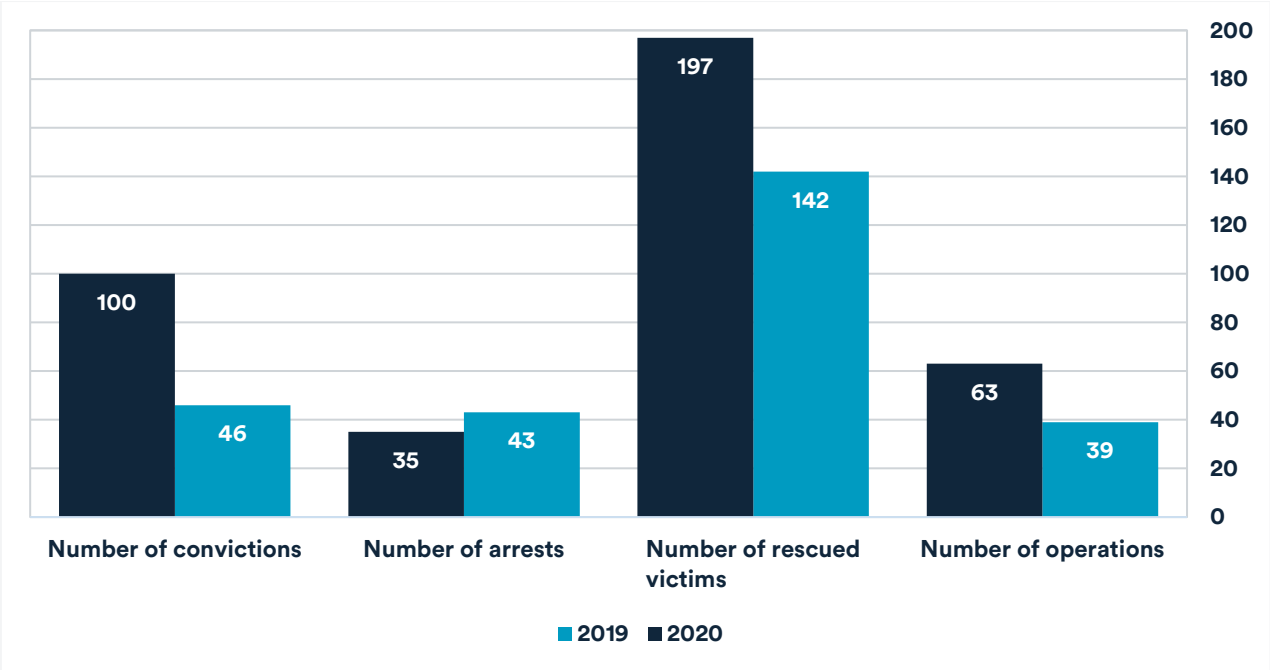
As outlined in section 2, the Philippines has several laws addressing child sexual abuse and exploitation, including OSEC. This includes the recently enacted OSAEC and CSAEM Act. However, it has been noted that the implementation of these laws in practice remains as an issue. For example, the UN Special Rapporteur on the sale and sexual exploitation of children, Mama Fatima Singhateh stated that:

> "Laws are very good but measures must also be put in place and it's one thing to have very well drafted laws and another to actually implement it and make sure that implementation trickles down to the grassroots level because many times we've seen in other countries where laws have been drafted but the implementation is weak." - (Bicol Express News, 2022).

In the Philippines, there are several different law enforcement agencies and authorities working on combatting OSEC. The Philippine National Police (PNP) and the National Bureau of Investigation are the two primary authorities involved in investigating and prosecuting OSEC cases (Aritao & Pangilinan, 2018, p. 223). In 2019, the Philippine Internet Crimes Against Children Center (PICACC) was also launched as a collective effort to combat child sexual exploitation across the Philippines in collaboration with the UK National Crime Agency and International Justice Mission (IJM) (Australian Federal Police, 2020).

As part of the intensified action against OSEC, the number of police operations conducted across the country increased by 61% in 2020, with 63 operations taking place in comparison to the 39 operations conducted in 2019. This spike in operations resulted in more victims being identified and rescued. In 2020, 197 victims were rescued—55 more than the 142 rescued in 2019 (Inter-Agency Council Against Trafficking, 2020, p. 31).

Figure 1: OSEC operations in the Philippines[3]



[3] *(Inter-Agency Council Against Trafficking, 2020).*

Operations carried out by law enforcement agencies in 2020 led to a dramatic increase in convictions for OSEC cases. The Inter-Agency Council Against Trafficking reported that the conviction rate for OSEC cases was 92% in 2020, with 53% of these convictions achieved through plea bargaining (2020, p.31). The number of OSEC convictions rose dramatically from 46 in 2019 to 100 in 2020, representing an increase of 117% (ibid).

2.1. Law enforcement agencies

The Philippine National Police (PNP) is designed to be a nationwide law enforcement organisation with specialised branches handling particular regions and types of criminal activity, such as sexual abuse of minors, offences against women, and counterterrorism operations (Australian Government Department of Foreign Affairs and Trade, 2021, p. 29). Newly recruited officers receive one year of basic training, followed by an additional three to six months of instruction in a particular subject. Despite the competence of the police, they are hindered by a lack of resources and capacity, as well as inadequate coordination with other organisations (ibid).

The PNP leads the investigation of the majority of OSEC cases. The Philippine government reported working together with various foreign governments—such as Australia, Ireland, Malaysia, the United Kingdom, and the United States—on investigations related to human trafficking, mainly concerning OSEC (US Department of State, 2022).

There are two specific divisions of the PNP focusing on the investigation of OSEC cases. These are the PNP Women and Children Protection Centre (PNP-WCPC) and PNP Anti-Cybercrime Group.

- The **PNP-WCPC** is the main agency in charge of dealing with cases of violence, exploitation, and abuse against women and children, as well as both CSEA and OCSEA (Aritao & Pangilinan, 2018, p. 23). The PNP-WCPC works together with the PNP Anti-Cybercrime Group and other law enforcement entities to identify individuals who are forcing children and young people into online child sexual exploitation and abuse. In 2016, The PNP-WCPC set up a division specifically dedicated to combatting Internet crimes against children in response to the increasing number of OCSEA cases (ECPAT, INTERPOL, and UNICEF, 2022, p. 88). This office is responsible for obtaining intelligence and acting on tips from foreign law enforcement organisations.
- The **PNP Anti-Cybercrime Group** is responsible for looking into any offences that are committed using information and communication technologies, including OSEC (Anti-Cybercrime Group, n.d.). This division carries out activities such as recovering data from seized devices, conducting forensic analysis, offering technical assistance to law enforcement, keeping an intelligence database up to date, setting up and running a digital forensic laboratory, and giving instruction in anti-cybercrime tactics (ECPAT, INTERPOL, and UNICEF, 2022, p. 88).

IJM's Casework Tracking and Management System Records identified that by June 2018, the PNP-WCPC conducted 39 child-protection activities that led to 56 arrests, 54 criminal cases, and the rescue of 133 OSEC victims. As a result of the operations of the PNP WCPC, 17 convictions were secured (Aritao & Pangilinan, 2018, p. 223).

In addition to the PNP, the National Bureau of Investigation (NBI) also operates in the field of human trafficking cases, including OSEC, through its Anti-Human Trafficking Division (AHTRAD) (Aritao & Pangilinan, 2018, p. 223). For example, AHTRAD conducted an operation in 2022 to arrest two human trafficking suspects involved in the making of child sexual and exploitative materials to sell overseas customers over the Internet (Maharlika TV, 2022). This operation helped rescue five child victims.

IJM's Casework Tracking and Management System Records found that by June 2018, the NBI had conducted 21 child-protection operations, resulting in 41 arrests, 48 criminal cases, and the rescue of 101 OSEC victims (Aritao & Pangilinan, 2018, p. 224). Eight convictions were handed down due to the NBI AHTRAD-related operations (ibid).

Table 4: Domestic Authorities working on investigation and prosecution of OSEC cases

<table>
<tr><td rowspan="4">Law Enforcement Agencies</td><td rowspan="2">Philippines National Police</td><td>Women and Children Protection Centre</td></tr>
<tr><td>• Has a specific mandate to investigate OSEC and other online sexual crimes against children.
• Has an Anti-Trafficking in Persons Division (ATIPD).
• Collaborates with Anti-Cybercrime Group and other law enforcement agencies.</td></tr>
<tr><td rowspan="2">National Bureau of Investigation</td><td>Anti-Cybercrime Group:</td></tr>
<tr><td>• Has a mandate to investigate all crimes committed through ICTs.
• Conducts data recovery and forensic analysis on devices seized by law enforcement agencies.
• Provides technical investigative assistance and training on anti-cybercrime operations.</td></tr>
<tr><td rowspan="2">Other Organisations</td><td colspan="2">Inter-Agency Council Against Child Pornography:</td></tr>
<tr><td colspan="2">• Established in 2010 with a mandate to manage, track, and oversee the implementation of the Anti-Child Pornography Act of 2009.
• Works closely with other intergovernmental organisations and national and international NGOs.
• Develops plans and programmes to curb child pornography and other online sexual exploitation and abuse of children.</td></tr>
<tr><td colspan="2">Philippine Internet Crimes Against Children Center:</td></tr>
<tr><td colspan="2">• Established in 2019 as a joint effort of the PNP, the Australian Federal Police, the UK National Crime Agency, and IJM.
• Helps investigate OSEC cases with the NBI and PNP-WCPC.
• Helps local law enforcement to gather digital evidence on OSEC.
• Serves as a platform for the stakeholders to address OSEC.</td></tr>
</table>

In 2010, the Inter-Agency Council Against Child Pornography was established with the primary objective of eliminating OCSEA through the management, tracking, and overseeing of the execution of the Anti-Child Pornography Act of 2009. It is responsible for forming extensive and unified plans and programmes to prevent and curb OCSEA and with synchronising the activities of its member organisations. It has the authority to direct other agencies to address incidents brought to their attention quickly and to report to the Council on the actions taken (ECPAT, INTERPOL, and UNICEF, 2022, p. 90).

In 2019, the Philippine Internet Crimes Against Children Center was created through a collaboration between the Philippines National Police, the Australian Federal Police, the National Crime Agency of the UK, and IJM to increase their efforts to deal with and prevent OCSEA in the Philippines (UK Crime, Justice and Law, 2019). The Center, which is part of the Directorate of Investigation and Detective Management, is responsible for investigating cases of OCSEA, in conjunction with the NBI and the PNP-WCPC. It helps local police officers and law enforcement units with digital evidence gathering, which is considered a major issue, and also provides a platform for stakeholders working on OCSEA to come together and discuss crime prevention strategies, plan priorities, and work together operationally (ECPAT, INTERPOL, and UNICEF, 2022, p. 87).

2.2. Investigation and prosecution challenges

There is a need for more staffing in law enforcement in the Philippines responsible for anti-trafficking, increased budget for operations, and improved instruments and expertise for digital evidence examination because of the large number of tips on cybercrime with regard to the sexual exploitation of children (US Department of State, 2022).

Law enforcement staff working on OSEC cases lack the required expertise due to frequent rotations. Rotating police officers too often and a lack of regular, consistent, and specialised instruction to incoming law enforcement personnel impedes the success of OSEC training programmes (ECPAT, INTERPOL, and UNICEF, 2022, p. 90). A Supreme Court judge participating in a study conducted by ECPAT, INTERPOL, and UNICEF stated that 'we really work hard to train prosecutors, police officers, but we get the news that they are transferred. And then we have to train new ones again and also with the judges' (2022, p.90). This issue has also been raised by an Assistant State Prosecutor from the Department of Justice, saying that 'in most organisations, just like the police here in the Philippines, the turnover of personnel from one organisation to the other is fast' (ibid). Such frequent rotation of staff has an impact on knowledge and skills of law enforcement personnel as highlighted by a lawyer stating that 'that's a big problem that we have, the shifting of the police officers. Instead of having them already trained, they would be assigned to another department, a new police officer would be there with no experience handling children' (ibid).

The Department of Justice and the PNP report that the investigation of OSEC cases poses significant challenges due to the lack of sufficient evidence to build a case against a suspected offender (ECPAT, 2020). Law enforcement struggle to obtain information and data from Internet Service Providers (ISPs) in the Philippines despite the fact that they are mandated by the laws to provide law enforcement agencies with the relevant OSEC data (ibid). ISPs argue that they could not comply with these laws because of technical limitations. Police Major Michael Virtudazo of the PNP explained this difficulty, noting that in order to request information and data from the ISPs, the police should first get a court warrant, however their lack of sufficient evidence against a suspected internet user at the start of the investigation is the very reason why they struggle to get that warrant (ibid).

3. Investigation of Financial Transactions in OSEC Cases

The evidence reviewed in this study and findings from interviews show that money transfers from demand-side to supply-side are usually made via money remittance centres in the Philippines (Interview #18). This is mostly because facilitators of OSEC in the Philippines usually dictate which payment platform should be used by the buyer to send the money (Interview #5). Neil Giles stated that:

> "The person who holds the cards at the end of the day is the perpetrator, the delivery side of the equation. The abuser is the person who says, I need that money in this form in this place. So, the challenge for the buyer is to either negotiate that differently, or conform. Similarly, that gives challenges to the purchaser, but the purchaser has a desire to access the material, so they will take a risk if they have to." - (Interview #7).

Usually, buyers of OSEC make low value payments to facilitators in the Philippines. Payments of this size are common in the context of the Philippines because a large number of Filipino migrant workers abroad send regular remittances to their families in the Philippines (Interview #1). However, what may be considered distinctive in OSEC cases is inconsistency in these transactions. For example, one participant underlined that if the money is sent by a migrant worker to their family, this usually takes a consistent form in terms of both amount and frequency (i.e., $30 every Friday). However, both the amount and the frequency may be inconsistent in OSEC cases (ibid). Irregular payments from the same country to the Philippines raise more suspicion, especially when there are no apparent family connections between the sender and receiver. In OSEC cases, money transfers typically involve one sender and multiple recipients. This pattern suggests that the sexually motivated offender seeks exploitation from multiple traffickers, with each trafficker receiving payments from multiple senders (Interview #3).

3.1. Use of financial transactions for investigative purposes

Participants in this study highlighted that financial transactions provide valuable intelligence, although they do not always directly lead to immediate arrests or convictions (Interview #3). In the context of law enforcement in the Philippines, financial data is most beneficial as a tool for targeting suspected offenders. For instance, when there is a significant number of digital reports indicating suspicious communication patterns between individuals in the Philippines and another country, but they are not viewable by the law enforcement, there is limited actionable information. However, when combined with records of financial transactions between the individuals in the Philippines and that country, a clearer and more suspicious picture emerges. Therefore, in terms of investigation, cases involving financial transactions are prioritised because they provide additional indicators of potential criminal activity (Interview #8). An IJM representative participating in this study emphasised that:

> "Financial data brings clarity to what is happening in this particular case and helps investigators focus on a case that maybe seems more severe or just easier to investigate. We are more likely to determine that this person is an offender versus the one who's sending or who's receiving payments every two weeks in the same amount from the same person and nobody else. That person is unlikely to be an offender in that sense. So it helps law enforcement focus their work and then they have to use other strategies to investigate the case and bring it to the point of rescuing a child and making an arrest. It's possible, then, after that arrest has been made and the defendant has been held pending trial, that the financial records could be introduced for additional charges as evidence of additional charges, depending on the electronic evidence found through the investigation, statements made by victims or other evidence that may be uncovered." - (Interview #3).

3.2. Monitoring financial transactions

As explained in section 2, the OSAEC and CSAEM Act and Anti-Money Laundering Act in the Philippines require financial institutions to monitor their services and report suspicious transactions to the AMLC. Eric Favila from the AMLakas Corporation emphasised that the Philippines has a notable gap in combatting OSEC due to the absence of active involvement from the financial services sector in monitoring and reporting essential intelligence on this matter (Interview #12).

Shauna Tomkins from the AMLakas Corporation explained that financial institutions in the Philippines do not generally monitor transactions under PHP 500,000 (Interview #13). She further emphasised that the range of transactions monitored does not capture low value money transactions made for OSEC. Therefore, Tomkins observed that 'the filter that they [financial institutions] put on their system meant that no one was even looking at these transactions' (ibid).

Study participants highlighted that when there is a mechanism to monitor and report suspicious transactions, it is not always effective and consistent. Local money remittance services operating in the Philippines do not generally check ID verification to establish the relationship between the sender and receiver (Interview #17). However, with the enactment of the OSAEC and CSAEM Act, money remittance services should require a valid ID and associate that ID to the person who is trying to withdraw the money (Interview #18). Although this is considered an improvement, participants highlighted the potential shortcomings in implementation of ID requirement in practice (Interview #13).

Financial institutions may also refrain from developing and implementing effective monitoring mechanisms because of the associated costs. For example, Shauna Tomkins from the AMLakas Corporation pointed that money remittance companies charge low value administering fees (Interview #13). Therefore, money remittance companies find it financially impractical to spend a substantial amount on investigating the legitimacy of transactions when they typically receive low values for administering payments (ibid).

The lack of effective monitoring systems cannot only be explained by associated costs because financial institutions usually have effective systems in place to monitor for fraud. Shauna Tomkins pointed out that although the majority of financial institutions are able to detect small amount transactions associated with fraud, this does not happen in the case of OSEC transactions (Interview #13). She stated that 'the only reason they [financial institutions] do fraud monitoring is because they wear the cost in fraud cases. So, they manage to do it for fraud, so why not these other transactions?' (ibid).

3.3. Cooperation with financial institutions

One police major interviewed for the Disrupting Harm project highlighted the importance of open data sharing and cooperation with the financial sector, including the Anti-Money Laundering Council, PayPal, and European money transfer services, to be able to investigate OSEC and other online sexual crimes against children more successfully (ECPAT, INTERPOL, and UNICEF, 2022, p. 89). This has become increasingly important when dealing with offenders based in other countries transferring money to facilitators in the Philippines (ibid).

On 14 December 2020, the Bangko Sentral ng Pilipinas issued Memorandum No. M-2020-092, which requests financial institutions bolster their risk management capabilities to tackle the emergence of transactions related to OSEC (Bangko Sentral ng Pilipinas, 2020). The memo demonstrated a diversity of practices among financial institutions, ranging from positive practices to areas that require urgent improvement. It was revealed that financial institutions are conscious of the risks that OSEC can bring to their operations (ibid).

The Bangko Sentral ng Pilipinas indicated that some financial institutions represented good practices in terms of setting a process of customer identification and verification, as well as utilising automated screening. Additionally, banks and other financial institutions that are part of the AMLC's Public Private Partnership Program (PPPP) have access to important data on customers connected to organised crime and other illegal activities, which can help in identifying customers or transactions that require further scrutiny for OSEC (ibid).

The Bangko Sentral ng Pilipinas has also pointed out the need to strengthen certain areas to reduce the possibility of money laundering related to OSEC activities, such as carrying out risk assessments, verifying customer information, keeping track of transactions, and reporting any suspicious activity (ibid). It is stated in the memo that the Board of Directors and Senior Management in the financial sector should set a proactive tone at the top and establish a culture of risk awareness and compliance within their organisations to ensure effective implementation of a robust framework that has the capacity to detect and mitigate risks arising from OSEC-related transactions (ibid).

In the Philippines, Suspicious Transaction Reports (STRs) related to OSEC are usually tagged as relating to the following laws:

- Anti-Trafficking in Persons Act of 2003 or Predicate Crime (PC) 19.
- Anti-Photo and Video Voyeurism Act of 2009 or PC30.
- Anti-Child Pornography of 2009 or PC31.
- Special Protection of Children Against Abuse, Exploitation and Discrimination" or PC32 (Bangko Sentral ng Pilipinas, 2020).

In terms of customer onboarding due diligence, the Bangko Sentral ng Pilipinas indicated that financial institutions have taken some actions. For example, customers are required to fill out a Customer Information Sheet (CIS) and present valid identification document. The CIS includes the required customer information. In some Money Service Businesses (MSBs), supplemental information such as the purpose of the remittance and relationship between parties of the transactions are also required (ibid, p. 4). It is also reported that certain financial institutions are employing automated customer risk profiling systems that are connected to their customer information onboarding systems. This allows for uniform and effective implementation in all branches. Some banking and financial services firms have implemented automatic tagging of customers as high risk based on pay-out locations that are notorious for involvement in OSEC activities, the presence of suspicious transaction patterns connected to OSEC, and the results of watchlist monitoring (ibid). MSBs also employ structured accreditation process for remittance sub-agents primarily focusing on Know Your Sub-Agent (KYSA) processes.

While some promising practices are emerging in the financial sector, some financial institutions failed to effectively implement the measures. For example, customer identification policies across branches and remittance partners were not consistently implemented in some areas. Further, a lack of sophistication in risk profiling techniques, characterised by manual processes and utilising few or inadequate factors, has led to implementation and audit trail issues. For some financial institutions, factors such as purpose, expected activity, amount, frequency, volume, and value of remittances are not taken into account when assessing risk. Further, supplemental information which could be useful for monitoring OSEC activities (e.g. country of origin, remitter's name and address, and the relationship between the parties to the remittance) is not gathered or used for customer risk profiling (ibid).

Bibliography

AMLC. (2020). *Online Sexual Exploitation of Children: A Crime with a Global Impact and an Evolving Transnational Threat*. Retrieved January 2023, from http://www.amlc.gov.ph/images/PDFs/2020%20AUG%20AMLC%20OSEC%20AN%20EMERGING%20RISK%20AMID%20THE%20COVID19%20PANDEMIC.pdf

Anti-Cybercrime Group. (n.d.). *Home*. Retrieved January 2023, from https://acg.pnp.gov.ph/main/

Aritao, B. L., & Pangilinan, J. S. (2018). Online Sexual Exploitation of Children: Applicable Laws, Casework Perspectives, and Recommendations. *Ateneo Law Journal, 63*(1), 185-236.

Australian Federal Police. (2020, March 11). *PICACC celebrates first year; firm in its resolve to end OSEC*. Retrieved January 2023, from https://www.afp.gov.au/news-media/media-releases/picacc-celebrates-first-year-firm-its-resolve-end-osec

Australian Government Department of Foreign Affairs and Trade. (2021). *DFAT Country Information Report : The Philippines*. Retrieved January 2023, from https://www.dfat.gov.au/sites/default/files/country-information-report-philippines.pdf

Bangko Sentral ng Pilipinas. (2020, December 14). *Memorandum No. M-2020-092: Guidance Paper on Managing Money Laundering Risks Related to Online Sexual Exploitation of Children (OSEC)*. Retrieved February 2023, from https://www.bsp.gov.ph/Regulations/Issuances/2020/m092.pdf

Bicol Express News. (2022, October 11). *PH still needs to fill gaps in response against sexual exploitation of children; UN Rapporteur says*. Retrieved January 2023, from http://bicolexpress.news/ph-still-needs-to-fill-gaps-in-response-against-sexual-exploitation-of-children-un-rapporteur-says/

Council of Europe. (n.d.). Internet Intermediaries. Retrieved July 2023, from https://www.coe.int/en/web/freedom-expression/internet-intermediaries#:~:text=The%20term%20'internet%20intermediaries'%20commonly,between%20natural%20and%20legal%20persons.

ECPAT. (2020, July 23). *From reactive to proactive: A local solution to the transnational crime of Online Sexual Exploitation of Children*. Retrieved January 2023, from http://ecpat.org.ph/2021/06/11/from-reactive-to-proactive-a-local-solution-to-the-transnational-crime-of-online-sexual-exploitation-of-children/

ECPAT France. (2022, May). *Deep Dive into the Phenomenon of Live Online Child Sexual Abuse and Exploitation: How to Better Protect Children?* Retrieved January 2023, from https://ecpat-france.fr/www.ecpat-france/wp-content/uploads/2022/06/Recherche-live-streaming_web.pdf

ECPAT International. (2021). *Execuitve Summary: Philippines*. Retrieved January 2023, from https://ecpat.org/wp-content/uploads/2021/08/EXSUM_A4A_EAP_PHILIPPINES-1.pdf

ECPAT, INTERPOL, and UNICEF. (2022). *Disrupting Harm in the Philippines: Evidence on online child sexual exploitation and abuse*. Retrieved January 2023, from Global Partnership to End Violence Against Children: https://ecpat.org/wp-content/uploads/2022/04/DH_Philippines_ONLINE_FINAL.pdf

European Financial Coalition. (2015). *Strategic Assessment 2014*. Retrieved January 2023, from https://www.europol.europa.eu/cms/sites/default/files/documents/efc_strategic_assessment_2014.pdf

IJM. (2020). *Online Sexual Exploitation of Children in the Philippines: Analysis and Recommendations for Governments, Industry, and Civil Society*. Retrieved January 2023, from https://ijmstoragelive.blob.core.windows.net/ijmna/documents/studies/Final-Public-Full-Report-5_20_2020_2021-02-05-055439.pdf

Inter-Agency Council Against Trafficking. (2020). *Accomplishment Report: For the Reporting Period: CY 2020*. Retrieved January 2023, from https://iacat.gov.ph/wp-content/uploads/2022/02/2020-IACAT-Annual-TIP-Report-2.pdf

International Centre for Missing & Exploited Children. (2021, October). *Philippines Legal Review Position Paper*. Retrieved January 2023, from https://cdn.icmec.org/wp-content/uploads/2021/12/Philippines-Legal-Review-Position-Paper_Final-signed_Oct2021-compressed-1.pdf

LexisNexis (n.d.) Internet Service Provider definition. Retrieved July 2023, from https://www.lexisnexis.co.uk/legal/glossary/internet-service-provider#:~:text=What%20does%20Internet%20Service%20Provider,capacity%20on%20a%20larger%20network.

Maharlika TV. (2022, September 27). *NBI arrests 2 human trafficking suspects; 5 minors rescued during operation*. Retrieved January 2023, from https://maharlika.tv/2022/09/27/nbi-arrests-2-human-trafficking-suspects-5-minors-rescued-during-operation/

Supreme Court of the Republic of the Philippines. (2014, February 14). *Disini v. The Secretary of Justice (G.R. No. 203335)*. Retrieved January 2023, from https://lawphil.net/judjuris/juri2014/feb2014/gr_203335_2014.html

The Exodus Road. (2022, March 15). *Human Trafficking in the Philippines*. Retrieved January 2023, from https://theexodusroad.com/human-trafficking-in-the-philippines/#:~:text=Human%20trafficking%20is%20the%20second,living%20as%20modern%2Dday%20slaves

UK Crime, Justice and Law. (2019, February 27). *Launch of the Philippine Internet Crimes Against Children Center*. Retrieved January 2023, from https://www.gov.uk/government/news/launch-of-the-philippine-internet-crimes-against-children-center

UNICEF Philippines. (2020). *National Study on Online Sexual Abuse and Exploitation of Children in the Philippines: Final Report*. Retrieved January 2023, from https://www.unicef.org/philippines/media/2711/file/UNIPH-2021-NationalStudyOSAEC-FullReport.pdf

US Department of State. (2022). *2022 Trafficking in Persons Report*. Retrieved January 2023, from https://www.state.gov/reports/2022-trafficking-in-persons-report/philippines__trashed/

Varrella, A. (2017). Live Streaming of Child Sexual Abuse: Background, Legislative Frameworks and the Experience of the Philippines. *ECPAT International Journal, 12*, 47-61.

Watson, L. (2021, October 13). *Month-old babies among Philippines' modern slavery victims as lockdown fuels exploitation pandemic*. Retrieved January 2023, from ITV: https://www.itv.com/news/2021-10-12/babies-among-modern-slavery-victims-as-lockdown-fuels-exploitation-pandemic

University of Nottingham
Rights Lab

GLOBAL FUND TO END MODERN SLAVERY

Discover more about our world-class research

nottingham.ac.uk/rights-lab

rightslab@nottingham.ac.uk

@rightsbeacon

Published in September 2023.